

## ABSTRACT OF THE DISCLOSURE

A system and method is provided for detecting, tracking and blocking denial of service (“DoS”) attacks, which can occur between local computer systems and/or between remote computer systems, network links, and/or routing systems over a computer network. The system includes a collector adapted to receive a plurality of data statistics from the computer network and to process the plurality of data statistics to detect one or more data packet flow anomalies. The collector is further adapted to generate a plurality of signals representing the one or more data packet flow anomalies. The system further includes a controller that is coupled to the collector and is adapted to receive the plurality of signals from the collector. The controller is constructed and arranged to respond to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source, and to block the one or more data packet flow anomalies using a filtering mechanism executed in close proximity to the at least one source.

DRAFT DRAFT DRAFT DRAFT